VALTIOVARAINMINISTERIÖ

Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelma

Valtiovarainministeriön julkaisu – 32/2018

Julkisen hallinnon ICT

Valtiovarainministeriön julkaisu 32/2018

Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelma

Valtiovarainministeriö, Helsinki 2018

Valtiovarainministeriö

ISBN: 978-952-251-975-7

Taitto: Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2018

Kuvailulehti

Julkaisija	Valtiovarainministeriö		Joulukuu 2018
Tekijät	Kimmo Rousku (toimittaja)		
Julkaisun nimi	Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelma		
Julkaisusarjan nimi ja numero	Valtiovarainministeriön julkaisu 32/2018		
Teema	Julkisen hallinnon ICT		
ISBN PDF	978-952-251-975-7	**ISSN PDF**	1797-9714
URN-osoite	http://urn.fi/URN:ISBN:978-952-251-975-7		
Sivumäärä	42	**Kieli**	Suomi
Asiasanat	VAHTI, riskienhallinta, tietoturva, tietosuoja, kyberturvallisuus, jatkuvuudenhallinta, digitaalinen turvallisuus		

Tiivistelmä

Valtiovarainministeriön tehtävänä on julkisen hallinnon tietoturvallisuuden yleinen kehittäminen ja valtionhallinnon tietoturvallisuuden ohjaus. Osana tätä kehittämistä ja ohjaustyötä valtiovarainministeriö kerää julkisen hallinnon organisaatioilta tietoa niin organisaatioiden turvallisuuden toteutumisesta kuin havaituista tai toteutuneista uhkista. Hallinnollisen tiedon ohella kerätään tietoa henkilöstön ja johdon ohjeistuksesta, koulutuksesta, osaamisesta ja asenteista. Tätä kokonaiskuvaa täydennetään organisaatioiden kriittisten palveluiden toimintaa ja turvallisuuden toteutumista mittaavilla tiedoilla. Tällä ohjauksella edistetään julkisen hallinnon tietoturvallisuutta, jonka avulla pyritään mahdollistamaan turvalliset, luotettavat palvelut.

Tämän tietopohjan, toimintaympäristössä havaittujen muutosten, ennustettavan uhkatilanteiden muutoksen sekä viimeisten vuosien aikana julkaistujen muiden raporttien ja ohjausasiakirjojen perusteella sekä ennakoiden tulevia lainsäädäntömuutoksia, valtiovarainministeriö on tunnistanut tarpeen julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelmalle. Kehittämisohjelman tavoitteena on varmistaa, että julkishallinnon digitaaliset palvelut toimivat ja että niihin luotetaan. Kehittämisohjelmaan on valittu tavoitteen mahdollistamiseksi kolme painoaluetta, jotka ovat 1) Digiturvallisuuden johtamisen ja riskienhallinnan kehittäminen, 2) Osaava henkilöstö sekä 3) Uuden teknologian hyödyntäminen palveluiden ja turvallisuuden toteuttamisessa. Nämä edellä olevat osa-alueet tulee ottaa huomioon myös tietoturvallisuuteen liittyvää arkkitehtuurityötä kehitettäessä ja sitä hyödynnettäessä. Näiden avulla luodaan ja kehitetään digiturvallista asennetta sekä mahdollistetaan uutta teknologiaa hyödyntäviä palveluita hallinnossa.

Kolmen valitun painoalueen kehittämiseksi valtiovarainministeriö toteuttaa julkisen hallinnon digitaalisen turvallisuuden toimenpideohjelman vuosille 2018-2021. Toimenpideohjelma koostuu viidestä toimenpiteestä, joiden avulla varmistetaan painoalueiden kehittyminen ja kehittämisohjelman tavoitteiden saavuttaminen. Valtiovarainministeriö voi tarjota organisaatioille uusia toimenpiteitä vuosittaisen kehittämisohjelman arvioinnin yhteydessä. Kehittämis- ja toimenpideohjelman laatimisesta ja ohjaamisesta vastaa valtiovarainministeriö. Väestörekisterikeskus vastaa kehittämisohjelman toimenpiteiden operatiivisesta tuottamisesta julkisen hallinnon käyttöön sekä niiden toteutumisen raportoinnista valtiovarainministeriöön ja VAHTIlle. Julkisen hallinnon organisaatiot vastaavat omalta osaltaan toimenpiteiden toteuttamisesta omassa toiminnassaan. Kehittämisohjelman avulla tuetaan myös Suomen Kyberturvallisuusstrategian ja sen toimeenpano-ohjelman toteutumista osana valtiovarainministeriön vastuulla olevia toimenpiteitä. Yhdessä näillä toimenpiteillä kehitetään myös julkisen hallinnon kyberturvallisuutta.

Kustantaja	Valtiovarainministeriö
Julkaisun myynti/ jakaja	Sähköinen versio: julkaisut.valtioneuvosto.fi Julkaisumyynti: julkaisutilaukset.valtioneuvosto.fi

Presentationsblad

Utgivare	Finansministeriet		December 2018
Författare	Kimmo Rousku (redaktör)		
Publikationens titel	Utvecklingsprogrammet för den digitala säkerheten inom den offentliga förvaltningen		
Publikationsseriens namn och nummer	Finansministeriets publikationer 32/2018		
Tema	Offentliga förvaltningens ICT		
ISBN PDF	978-952-251-975-7	**ISSN PDF**	1797-9714
URN-adress	http://urn.fi/URN:ISBN:978-952-251-975-7		
Sidantal	42	**Språk**	Finska
Nyckelord	VAHTI, riskhantering, informationssäkerhet, datasäkerhet, cybersäkerhet, kontinuitetskontroll, digital säkerhet		

Referat

Finansministeriet svarar för det allmänna utvecklandet av informationssäkerheten inom den offentliga förvaltningen och för styrandet av informationssäkerheten inom statsförvaltningen. Finansministeriet insamlar i anslutning till detta information från organisationerna inom den offentliga förvaltningen såväl om förverkligandet av säkerheten som om observerade eller realiserade hot. Utöver administrativ information insamlas information om personalens och ledningens anvisningar, utbildning, kompetens och attityder. Denna övergripande bild kompletteras med information som mäter funktionen hos organisationernas kritiska tjänster och förverkligandet av säkerheten. Denna styrning främjar informationssäkerheten inom den offentliga förvaltningen, som syftar till att möjliggöra säkra, pålitliga tjänster.

Finansministeriet har på basis av detta informationsunderlag, förändringarna i verksamhetsomgivningen, den förutsägbara förändringen av hotsituationerna samt andra rapporter och styrningsdokument som utgivits under de senaste åren, samt med hänsyn till kommande lagstiftningsändringar identifierat behovet av att inrätta ett program för utvecklandet av den digitala säkerheten inom den offentliga förvaltningen. Målet med utvecklingsprogrammet är att se till de digitala tjänsterna är driftssäkra och att användarna litar på dem. För att målet ska kunna uppnås har man valt tre tyngdpunktsområden för programmet: 1) Utveckling av ledandet av digital säkerhet och riskhantering, 2) Kompetent personal och 3) Utnyttjandet av ny teknik vid förverkligandet av tjänster och säkerhet. Dessa ovan nämnda delområden måste tas i beaktande även vid utvecklandet och utnyttjandet av arkitekturarbete som har ett samband med informationssäkerheten. Med hjälp av dessa kan man skapa och utveckla en positiv attityd gentemot digital säkerhet och möjliggöra tjänster som utnyttjar ny teknik.

Finansministeriet genomför åtgärdsprogrammet för digital säkerhet inom den offentliga förvaltningen under åren 2018-2021 i syfte att utveckla de tre prioriterade områdena. Åtgärdsprogrammet består av fem åtgärder med vilkas hjälp man säkerställer att de prioriterade områdena utvecklas och att utvecklingsprogrammets målsättningar uppnås. Finansministeriet kan erbjuda organisationerna nya åtgärder i samband med utvärderingen av det årliga utvecklingsprogrammet. Finansministeriet svarar för utarbetandet och styrningen av utvecklings- och åtgärdsprogrammet. Befolkningsregistercentralen svarar för den operativa produceringen av åtgärderna inom utvecklingsprogrammet och rapporterar om förverkligandet av dem till finansministeriet och VAHTI. Organisationerna inom den offentliga förvaltningen svarar för egen del för att åtgärderna genomförs i den egna verksamheten. Utvecklingsprogrammet stöder även förverkligandet av Finlands cybersäkerhetsstrategi och verkställighetsprogrammet för det. Dessa åtgärder utvecklar tillsammans cybersäkerheten inom den offentliga förvaltningen.

Förläggare	Finansministeriet
Distribution/ beställningar	Elektronisk version: julkaisut.valtioneuvosto.fi Beställningar: julkaisutilaukset.valtioneuvosto.fi

Description sheet

Published by	Ministry of Finance		December 2018
Authors	Kimmo Rousku		
Title of publication	Development Programme for Digital Security in Public Administration		
Series and publication number	Ministry of Finance publications 32/2018		
Subject	Public sector ICT		
ISBN PDF	978-952-251-975-7	**ISSN (PDF)**	1797-9714
Website address (URN)	http://urn.fi/URN:ISBN:978-952-251-975-7		
Pages	42	**Language**	Finnish
Keywords	Government Information Security Management Board (VAHTI), risk management, information security, data protection, cyber security, continuity management, digital security		

Abstract

The Ministry of Finance is responsible for the general development of information security in Finland's public administration and for overseeing information security in central government administration. As part of this development and oversight work, the Ministry of Finance gathers a range of information from organisations within the public administration, concerning for instance security and threats that have been detected or have materialised. Besides administrative information, the ministry also collects information on the guidance issued to personnel and management, the training given, and skills and attitudes. This overall view is supplemented by information measuring the activity of critical services in the various organisations and the extent of security in place. The oversight work serves to promote information security in public administration, with the aim of enabling the provision of secure and reliable services.

The Ministry of Finance identified a need for the development programme on the basis of the information gathered, observations of changes in the operating environment, the foreseeable change in threat scenarios, and other reports and guidance documents published in recent years, and by anticipating future amendments to legislation. The goal of the development programme is to ensure that digital services in public administration function well and can be relied on. To achieve this goal, three priority areas were selected for the programme: 1) managing digital security and enhancing risk management; 2) ensuring skills among personnel; 3) using new technology effectively in services and security. Attention must also be given to these priority areas when developing and using the information security architecture. The priority areas allow the creation and nurturing of a culture of digital security and also encourage government services that make use of new technology.

To further develop the three priority areas, the Ministry of Finance is putting in place an Action Plan for Digital Security in Public Administration in 2018–2021. The action plan consists of five measures for ensuring the further development of the priority areas and for achieving the aims of the development programme. New measures can then be offered to organisations by the Ministry of Finance in connection with the annual assessment of the development programme. The drafting of the development programme and action plan and the oversight of their implementation are the responsibility of the Ministry of Finance. The Population Register Centre is responsible for the practical implementation of the measures for the public administration and for reporting on this to the Ministry of Finance and to the Government Information Security Management Board (VAHTI). The organisations in the public administration are themselves responsible for implementation of the measures within their own operations. The development programme also supports Finland´s Cyber Security Strategy and the programme for putting that strategy into effect, as part of the measures for which the Ministry of Finance is responsible. Together, these measures also serve to develop cyber security in Finland's public administration.

Publisher	Ministry of Finance
Distributed by/ Publication sales	Online version: julkaisut.valtioneuvosto.fi Publication sales: julkaisutilaukset.valtioneuvosto.fi

Sisältö

LUKIJALLE

Valtiovarainministeriön tehtävänä on julkisen hallinnon tietoturvallisuuden yleinen kehittäminen ja valtionhallinnon tietoturvallisuuden ohjaus. Tämän julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelman avulla halutaan mahdollistaa, että Suomi säilyttää asemaansa digitaalisen turvallisuuden kärkijoukoissa. Samoin tällä mahdollistetaan, että julkisen hallinnon organisaatiot pystyvät tarjoamaan jatkossakin yhteiskunnan ja kansalaisten käyttöön turvallisia ja luotettavia palveluita. Lisäksi digitaalisen turvallisuuden avulla mahdollistetaan uuden teknologian turvallinen käyttöönotto ja hyödyntäminen.

Tällä julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelmalla valtiovarainministeriö ohjaa julkista hallintoa toteuttamaan laadittua myös turvallisuuskentän kattavaa kokonaisarkkitehtuuria noudattavia palveluratkaisuja ja siten digitaalista turvallisuutta kiinteänä, tärkeänä osana johtamista, riskienhallintaa, osaamisen kehittämistä sekä hallinnon kehittämistä ja toimintaa. Digitaalisen turvallisuuden kehittäminen on edellytys yhteiskuntamme toimintojen ja palveluiden laadulle ja turvallisuudelle, tehokkuudella ja avoimuudelle, sidosryhmien ja kansalaisten luottamukselle hallinnon toimintaan sekä kansalaisten ja yhteisöjen eduille ja oikeuksille.

Tämä kehittämisohjelma on tarkoitettu kaikille julkisen hallinnon organisaatioille ja sen toimeenpano organisaatiossa on organisaation johdon vastuulla. Kehittämisohjelma on osoitettu organisaation johdolle, jonka vastuulla on digitaalisen turvallisuuden eri osa-alueiden kokonaisvastuu. Johdon tehtävänä on delegoida näiden osa-alueiden vastuu organisaatiossa sekä antaa käyttöön tarvittavat resurssit sekä seurata kokonaisuuden etenemistä. Tämä koskee myös tätä kehittämisohjelman toteuttamista.

Jokaisen julkisen hallinnon organisaation tulee huolehtia siitä, että sen toiminnan kriittisyyden ja sille muuten asetettujen tavoitteiden mukainen digitaalinen turvallisuus sekä henkilötietojen suoja toteutuvat organisaatiossa, sen tuottamissa ja käyttämissä palveluissa sekä yhteistyössä sidosryhmien kanssa ja hankittaessa palveluita organisaation ulkopuolelta. Tällöin kehittämisessä tulee huolehtia toimenpiteistä, joilla pyritään ennakoivasti estämään tietoturvaloukkausten todennäköisyyttä ja vaikutusta,

mutta kuitenkin samalla kehittää myös suunnitelmia ja prosesseja, joilla tällaisten tapahtumien ilmetessä, organisaatiolla on kyky palautua normaaliin toimintaan.

Turvallisuuden toteuttaminen on esimerkiksi toiminnan johtamista, viestintää, henkilöstön osaamista, toimittajaketjujen hallintaa, kokonaisarkkitehtuurin noudattamista sekä teknologiaratkaisuja. Osaava henkilöstö toimii organisaation keskeisenä voimavarana ja turvallisuuden mahdollistajana. Henkilöstön osaaminen ja sitä kautta syntyvä turvallisuuskulttuuri ja –asenne ovat merkittävässä roolissa turvallisuuden toteuttamisessa ja luottamuksen rakentamisessa organisaatiossa ja sen sidosryhmissä. Tässä organisaation johdolla on keskeinen merkitys näiden muodostumisessa ja omalta osaltaan esimerkkinä toimimisessa.

Digitaalisen turvallisuuden toteuttaminen vaatii laaja-alaista yhteistyötä, jossa tarvitaan entistä parempaa viranomaisten, mutta myös palveluiden tuottamiseen osallistuvan verkoston (palveluiden toimittajat, alihankkijat) yhteistyötä.

Kehittämisohjelman tueksi on laadittu toimenpide-ohjelma, joka sisältää yhteensä viisi toimenpidettä, joihin organisaation tulee osallistua vuosien 2019-2021 aikana omaan aikatauluunsa ne sovittaen. Tämän kehittämisohjelman etenemisen seuranta ja vaikutusten mittaaminen sekä raportointi sisällytetään osaksi valtiovarainministeriön suorittamia julkisen hallinnon digitaalisen turvallisuuden kokonaiskuvan keräämistä.

Helsingissä 10.12.2018,

Anu Vehviläinen
Kunta- ja uudistusministeri

Anna-Maija Karjalainen
VAHTIn puheenjohtaja
ICT-johtaja, ylijohtaja

1 Digitaalinen toimintaympäristö muutoksessa

Mitä digitaalinen turvallisuus käsittää?

Valtiovarainministeriö on ottanut käyttöön termin digitaalinen turvallisuus kuvamaan tätä laaja-alaista kokonaisuutta, joka koostuu seuraavista keskeisistä turvallisuuteen liittyvistä osa-alueista:

1) Digiturvallisuuden johtaminen ja riskienhallinta

   Digitaalisen turvallisuuden johtamisen toteuttaminen sekä tätä tukeva riskienhallintamalli. Organisaatiossa käytössä oleva prosessi ja menetelmä, jonka avulla se varmistaa organisaation toiminnan tavoitteiden saavuttamisen sekä tunnistaa ja hallitsee sen jatkuvaan toimintaan liittyviä uhkia ja riskejä.

2) Toiminnan jatkuvuus ja varautuminen

   Organisaation toiminnan varmistaminen varautumalla ennakoivasti erilaisiin häiriötilanteisiin ja poikkeamiin tarvittavalla suunnittelulla ja suunnitelmilla (esimerkiksi jatkuvuus-, valmius- ja toipumissuunnittelu) mahdollistaen toiminnan palautuminen sen kriittisyyden huomioiden takaisin vaadittavalle tasolle.

3) Tietoturvallisuus

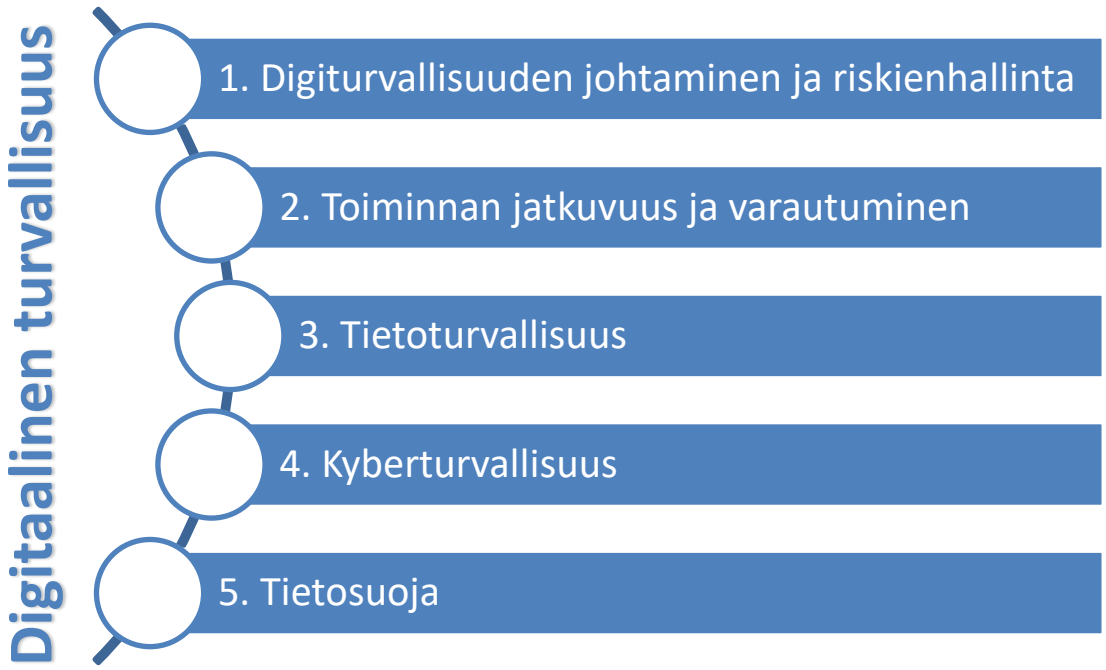
   Organisaation tunnistamien suojattavien kohteiden saatavuuden, eheyden ja luottamuksellisuuden varmistaminen.

4) Kyberturvallisuus

   Tila, jossa sähköisessä muodossa olevan datan tai informaation käsittelyyn tarkoitetuista tietojärjestelmistä yhteiskunnan elintärkeille toiminnoille tai muille näistä ympäristöistä riippuvaisille toiminnoille koituvat uhkat ja riskit ovat hallinnassa. Tähän kuuluvat lisäksi toimenpiteet, joilla voidaan ennakoivasti hallita ja tarvittaessa sietää erilaisia kyberuhkia (resilienssi) ja niiden vaikutuksia. Tietoturvasta huolehtimisen lisäksi kyberturvallisuuteen pyritään mm. toimenpiteillä, joiden tarkoituksena on turvata häiriytyneestä tietojärjestelmäympäristöstä riippuvaiset fyysisen maailman toiminnot.

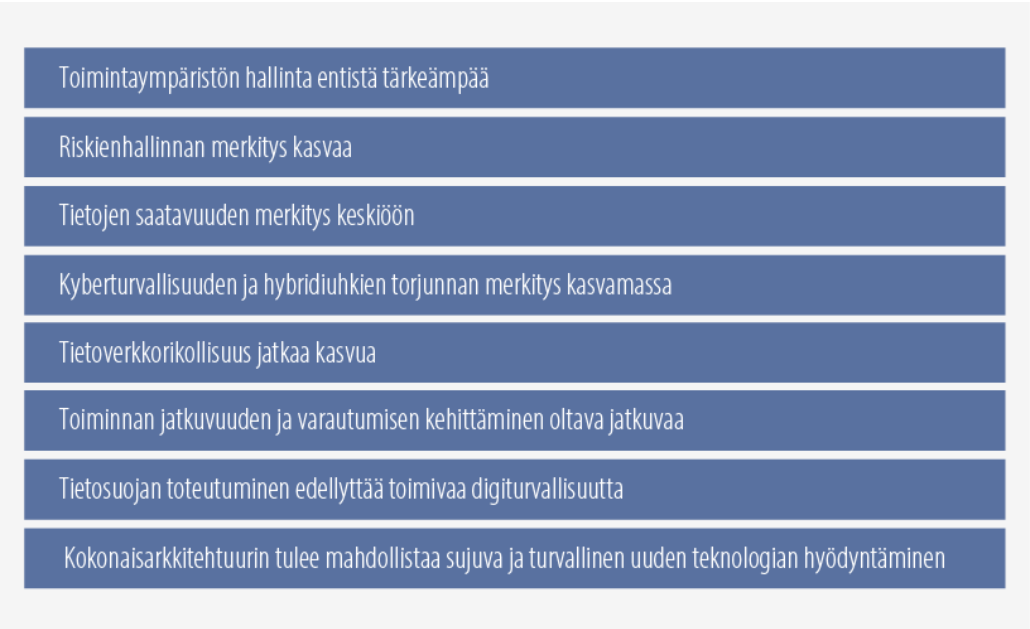
5) Tietosuoja

Perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä.



Kuva 1. Digitaalinen turvallisuus toimii sateenvarjona keskeisillä, digitaalisen toimintaympäristön toiminnan mahdollistaville ja sen turvaaville osa-alueille.

Valtiovarainministeriö kerää julkisen hallinnon organisaatioilta tietoa niin organisaatioiden turvallisuuden toteutumisesta kuin havaituista tai toteutuneista uhkista. Hallinnollisen tiedon ohella kerätään tietoa henkilöstön ja johdon ohjeistuksesta, koulutuksesta, osaamisesta ja asenteista. Tätä kokonaiskuvaa täydennetään organisaatioiden kriittisten palveluiden toimintaa ja turvallisuuden toteutumista mittaavilla tiedoilla. Tämän tietopohjan, toimintaympäristössä havaittujen muutosten, ennustettavan uhkatilanteiden muutoksen sekä viimeisten vuosien aikana julkaistujen muiden raporttien ja ohjausasiakirjojen avulla valtiovarainministeriö on tunnistanut muun muassa seuraavia keskeisiä digitaalisen toimintaympäristöön ja sen turvallisuuteen vaikuttavia tekijöitä:



Kuva 2. Kehittämisohjelman laatimisessa on valtiovarainministeriön toteuttamien kyselyiden ja mittareiden perusteella sekä asiantuntijaryhmän avulla tunnistettu kahdeksan osa-aluetta, jotka on otettu huomioon sen laatimisessa. Digitaalinen toimintaympäristö, uudet teknologiat ja palvelut tarjoavat valtavia mahdollisuuksia, mutta samassa yhteydessä niihin liittyvien uhkien tunnistaminen ja riskienhallinta on edellytys näiden uusien mahdollisuuksien valjastamiselle.

1.1 Toimintaympäristön hallinta entistä tärkeämpää

Toimimme verkostoituneessa yhteiskunnassa osana globalisoituvaa maailmaa. Yksittäisten tietojärjestelmien tilalle palveluiden taustalla toimivat yhä laajemmat digitaalisten palveluiden ekosysteemit, jotka muodostavat entistä laajempia palveluketjuja ja –alustoja. Laajan palvelukokonaisuuden toteuttamisessa saatetaan tarvita kymmeniä alihankkijoita.

Julkisessa hallinnossa on palveluita, joihin kohdistuu erityisiä turvallisuusvaatimuksia, kuten häiriönsieto vakavissa kriisitilanteissa. Lisäksi tiettyjen tietojen käsittelyn suojaamiseen liittyy kansallisia ja kansainvälisiä erityisvaatimuksia. Tietojenkäsittelyn ja toimintojen muuttuessa verkottuneemmaksi, tietojenkäsittely-ympäristöt edellyttävät laajempaa kokonaissuunnittelua. Suunnittelussa tulee pystyä huomioimaan eri toimijoiden tarpeet varmistaen ratkaisujen yhteensopivuus ja kustannustehokkuus.

Nopeassa muutoksessa oleva toimintaympäristö edellyttää aktiivista uhkien seurantaa ja riskienhallintaa, joiden avulla organisaatio pystyy varmistamaan tarkoituksenmukaisen turvallisuuden kehittämisen osana sen jokapäiväistä toimintaa. Tässä mallissa entistä tärkeämmäksi nousevat verkostossa toimivien tahojen välinen luottamus, yhteistyö sekä vastuunjaosta sopiminen.

Julkisessa hallinnossa on tapahtunut 2010-luvulla useita merkittäviä hallinnollisia rakennemuutoksia, joiden johdosta sekä ICT-palveluiden tuottaminen sekä julkisen hallinnon käyttöön tarkoitetut palvelut ovat uudistuneet merkittävästi. Uudet tai osin vielä kehitteillä olevat palvelukeskukset tai muu toimijat vastaavat keskitettyjen palveluiden tuottamisesta käyttäen joko omaa palvelutuotantoa ja henkilöstöä tai hyödyntäen markkinoilta saatavia palveluita ja alihankkijoita. Samanaikaisesti julkisessa hallinnossa, koko yhteiskunnassa on käynnissä merkittävä toimintatapojen uudistus rakentamalla ja muotoilemalla palveluita uudelleen asiakaslähtöisesti hyödyntäen uuden teknologian tarjoamia mahdollisuuksia.

Julkishallinnon palvelujen keskittämisellä saadaan merkittäviä kustannus- ja käytettävyyshyötyjä, mutta entistä enemmän tulisi myös arvioida keskittämiseen liittyviä riskejä (kasautumisriski) ja varautua niihin erityisesti digitaalisessa toimintaympäristössä toimittaessa. Kasautumisriskien kartoittaminen, arvioiminen ja johtaminen vaativat laaja-alaista yhteistyötä julkishallinnossa. Kasautumisriskejä tulee arvioida myös muiden kuin oman organisaation näkökulmasta ja myös käytetyillä alihankkijoilla on merkittävä rooli tässä asiassa.

Muuttuvassa toimintaympäristössä riippuvuuksia on kartoitettava ja arvioitava jatkuvaluonteisesti, jotta muutosten vaikutuksiin voidaan varautua ja voidaan selvittää sekä huomioida omaan toimintaan liittyvät merkittävät riippuvuudet muista toimijoista (tai viestiä muille toimijoille ennakolta).

Palveluiden hyödyntäessä yhä enemmän teknologioita, niiden muutosvauhti kasvaa. Julkisia palveluita tarjotaan yhä enemmän yhteistyössä eri toimijoiden kanssa. Palvelut voivat olla keskenään riippuvaisia ja palvelutuotanto voi koostua hankinta- ja tuotantoverkostoista. Yhteisissä palveluissa muutosten ja häiriöiden vaikutusten arviointi edellyttää riittävää kokonaiskuvaa. Palvelut voivat edellyttää myös yhteisiä toiminta- ja käyttösääntöjä turvallisuuden varmistamiseksi. Samalla tulisi kuitenkin voida varmistaa kustannustehokas toiminta.

Pilvipalvelujen käyttämiseen liittyy useita digitaalisen turvallisuuden kannalta olennaisia tekijöitä, jotka julkishallinnon organisaatioiden tulisi huomioida suunnitellessaan digitaalisten palvelujen viemistä pilveen. Näiden osalta julkishallinnon käyttöön luodaan yhteiset linjaukset ja käytännöt esimerkiksi siitä, miten pilvipalveluja käytetään ja minkälaisia palveluja sekä tietoa pilvipalveluihin on mahdollista viedä.

1.2 Riskienhallinnan merkitys kasvaa

Valtiovarainministeriö julkaisi OECD:n laatiman ”Digitaaliseen turvallisuuteen kohdistuvien riskien hallinta taloudellisen ja yhteiskunnallisen hyvinvoinnin edistämiseksi” [1] suosituksen syksyllä 2016. Tässä suosituksessa nostetaan esille digitaalisen toimintaympäristön mukanaan tuomat haasteet.

Suosituksen mukaan ”Digitaaliseen turvallisuuteen kohdistuvien uhkien ja poikkeamien määrä on kasvanut viime vuosina sekä johtanut merkittäviin taloudellisiin ja sosiaalisiin seurauksiin niin julkisille ja yksityisille organisaatioille kuin yksilöillekin. Tällaisia ovat esim. toiminnan keskeytyminen (palvelunestohyökkäyksen tai sabotaasin seurauksena), välittömät taloudelliset tappiot, oikeusjutut, maineelle aiheutuva vahinko, kilpailukyvyn menettäminen, (esim. liikesalaisuuksien anastuksen yhteydessä) sekä asiakkaiden luottamuksen menetys.”

Samoin riskienhallinnan merkitys on noussut sekä EU:n yleisen tietosuoja-asetuksen johdosta. Lisäksi valtiovarainministeriössä valmistelussa olevassa tiedonhallintalaissa edellytetään riskienhallinnan kehittämistä ja etenkin organisaatioilta kyvykkyyttä jäännösriskien käsittelyyn. Mikään organisaatio ei pysty digitaalisessa toimintaympäristössä toteuttamaan 100% turvallisuutta, joten toimiva riskienhallinta on nykyaikana välttämättömyys.

1.3 Tietojen saatavuuden merkitys keskiöön

Toiminnan aluksi sähköistyessä ja nyt uusia toimintamalleja digitalisoimalla tiedon saatavuuden merkitys on kasvanut. Keskeinen muutostekijä tässä on lisäksi tiedon määrän kasvaminen sekä tarve hyödyntää eri toimijoiden keräämiä ja tietoja entistä tehokkaammin. Koska kansalaisten, asiakkaiden ja muiden sidosryhmien tapa asioida on myös muuttunut 2010-luvulla uuden teknologian (uudenlaiset palvelut, mobiilit tietoliikenneyhteydet, päätelaitteet) ansiosta ajasta ja paikasta riippumattomaksi, palveluiden täytyy olla saatavilla käytännössä 24/7, vaikka organisaation ei alun perin tällaista palveluvelvoitetta ole tunnistanut. Tiedon saatavuuden mahdollistaminen edellyttää samalla sen eheydestä ja salassa pidettävien tietojen osalta niiden luottamuksellisuuden huolehtimisesta.

[1] http://julkaisut.valtioneuvosto.fi/handle/10024/75412

1.4 Kyberturvallisuuden ja hybridiuhkien torjunnan merkitys kasvamassa

Perinteisen, vakiintuneen tietoturvallisuuden rinnalle on 2010-luvulla noussut kyberturvallisuuteen liittyvä käsite, joka kuvastaa samalla hyvin toimintaympäristöön kohdistuvissa uhkissa tapahtunutta muutosta. Kyberturvallisuuden avulla pyritään huolehtimaan sähköisen, digitaalisen toimintaympäristön kokonaisturvallisuudesta. Tämä kattaa digitaalisessa toimintaympäristössä olevien tietojen ja palveluiden tietoturvallisuuden ohella myös tarvittavan muun, etenkin kriittisen infrastruktuurin (esimerkiksi energian tuotanto ja jakelu, tietoyhteiskunnan palvelut, logistiikka sekä finanssiala) toiminnan mukaan luettuna toiminnassa tarvittavan henkilöstön.

Muutaman viimeisen vuoden aikana esille ovat nousseet myös hybridivaikuttaminen sekä hybridiuhat uutena kyberturvallisuutta sivuavana kokonaisuutena. Hybridivaikuttamisessa yhdistyvät perinteiset ja uudet vaikuttamisen keinot, esimerkiksi tässä yhteydessä voidaan käyttää erilaisia psykologisia, poliittisia, taloudellisia, teknisiä, humanitaarisia ja sotilaallisia keinoja. Keskeistä hybridivaikuttamiselle on avainhenkilöihin kohdistuva psykologinen vaikuttaminen sekä informaatiovaikuttaminen. Erityisesti informaatiovaikuttaminen voi sisältää mm. suoria kyberhyökkäyksiä tai tarkoituksellisesti harhaanjohtavan tiedon levittämistä käyttäen erilaisia digitaalisia toimintaympäristön tarjoamia palveluita.

1.5 Tietoverkkorikollisuus jatkaa kasvua

[2]Tutkimusten mukaan kyberrikollisuuden vaikutus talouteen viisinkertaistui vuosien 2013 ja 2017 välillä, ja se voi edelleen nelinkertaistua vuoteen 2019 mennessä. Tietoverkko- ja kyberrikollisuus sekä muut ryhmät hakevat koko ajan uusia keinoja saavuttaa taloudellista hyötyä. Tätä varten luodaan uusia hyökkäys- ja väärinkäyttö- sekä huijauskeinoja, joita kohdistetaan kaikkiin organisaatioihin ja käyttäjiin. Suomi tai meillä toimivat yritykset, julkisen hallinnon organisaatiot, käyttäjät tai kansalaiset ovat kohteina tässä globaalissa tietoverkko- ja kyberrikollisten verkostossa.

Käytännössä emme voi itse juuri vaikuttaa siihen, olemmeko miten erilaisten hyökkäys- tai huijauskampanjoiden kohteita, sen sijaan voimme vaikuttaa siihen, kuinka hyvin pystymme niitä omassa digitaalisessa toimintaympäristössä havainnoimaan ja

[2] http://europa.eu/rapid/press-release_IP-17-3193_fi.htm

sen jälkeen niihin reagoimaan. Erityisesti havainnointikyvyn kehittäminen on keskeinen kyvykkyys, jonka avulla organisaatio saa paremman kokonaiskuvan oman organisaation turvallisuuden tilanteesta.

1.6 Toiminnan jatkuvuuden ja varautumisen kehittäminen oltava jatkuvaa

Turvallinen yhteiskunta edellyttää, että julkisen hallinnon toiminta on turvallista ja digitaalisten palveluiden käyttö luotettavaa. Vaikka Suomessa havaitaan suhteellisen harvoin merkittäviä tietoturvaloukkauksia tai muita yhteiskunnan toimintaa häiritseviä tapauksia, tulee turvallisuuden eri osa-alueisiin panostaa. Hallinnon toimintojen ja palvelujen digitalisaation myötä erilaisten toiminnallisten sekä häiriötapausten hallinnan tarve on korostunut. Kyberuhkien kasvu ja monimuotoistuminen on muuttanut kehittämisen painopistettä.

Valtiovarainministeriön keräämä aineisto osoittaa sen, että digitaaliseen toimintaympäristöön kohdistuvat niin tekniset häiriöt kuin tieto- ja kyberturvallisuuteen vaikuttavat poikkeamat tulevat yleistymään ja niiden vaikutus laajentumaan. Tällaisten häiriö- ja vikatilanteiden hallintaa tulee kehittää organisaatiotasolla sen toiminnan kriittisyys huomioiden.

Tämä tapahtuu sekä ennakoivasti, mahdollisia uhkia tunnistamalla ja estämällä niiden syntyminen ennen kuin ne pääsevät vaikuttamaan toimintaan sekä kehittämällä varautumista ja valmiutta reagoida tällaisiin tilanteisiin toiminnan kriittisyyden edellyttämällä tavalla.

1.7 Tietosuojan toteutuminen edellyttää toimivaa digiturvallisuutta

Valtaosa useimpien viranomaisten tietojenkäsittelyä liittyy henkilötietoihin. On olemassa viranomaisia, jotka eivät käsittele niitä muuta kuin oman organisaation henkilöstön osalta, mutta tällöinkin tällainen organisaatio saa käyttöönsä osana muuta yhteistyötä muiden osapuolien esimerkiksi asiakas- tai muita yritystietoja. Käytännössä henkilötietojen, siten tietosuojan merkitys on kasvussa myös 2020-luvulla.

EU:n yleinen tietosuoja-asetus sekä kansallinen lainsäädäntö muuttavat henkilötietojenkäsittelyyn liittyvää sääntelyä. Myös tässä yhteydessä digiturvallisuudella on keskeinen rooli; se toimii henkilötietojen turvallisen käsittelyn mahdollistajana.

1.8 Kokonaisarkkitehtuurin tulee mahdollistaa sujuva ja turvallinen uuden teknologian hyödyntäminen

Teknologian kehittyminen on nopeutunut erityisesti 2010-luvulla. Tämä koskee niin palveluiden tuotantomalleja, käytettävissä olevia päätelaitteita sekä tietoliikenneyhteyksiä. Yhteiskunnassa sekä globaalissa toimintaympäristössämme on meneillään teknologian tarjoamien mahdollisuuksien myötä yhä nopeutuva mahdollisuus uudistaa ja kehittää toimintaa innovatiivisilla, merkittävästi uudistavilla tavoilla. Tämä korostuu uusia ekosysteemejä, alustoja luovassa ja hyödyntävässä sekä automatisaatiota, robotisaatiota ja tekoälyä entistä tehokkaammin käyttöönottavassa yhteiskunnassa. Muutoksessa on keskeistä pyrkiä ymmärtämään ja tarvittaessa ennakoimaan vaikutuksia.

Uuden teknologian hyödyt saadaan käyttöön noudattamalla laadittua kokonaisarkkitehtuuria ja toteuttamalla hallitusti digitaalisten palvelujen käytettävyys- ja turvallisuusvaatimusten mukaiset yhteys-, integraatio- ja muut alustapalvelut.

Tästä muutoksesta hyvä esimerkki on käyttöpalveluiden ja muiden ICT-palveluiden ulkoistaminen ja siirtyminen käyttämään uudenlaisia palvelutuotantomalleja, esimerkiksi jaettua kapasiteettia hyödyntäviä malleja tai vielä laajamuotoisempia ns. ”pilvipalveluita”.

Päätelaitteiden muuttuminen tulee jatkumaan kiihtyvällä vauhdilla; mobiililaitteista on tullut yhä suorituskykyisempiä ja samoin niiden käytössä olevat tietoliikenneverkot tarjoavat yhä suurempia siirtonopeuksia, tosin vaihteluväli on hyvin suuri alueellisesti ja suorituskyky riippuu muutenkin verkon kuormituksesta.

Tietojenkäsittelykyvyn ja tietoliikenneyhteyksien tuominen tapahtuu osaksi kaikkia laitteita, jotka toimivat sähköllä. Jatkossa yhä useampi, jossain vaiheessa kaikki sähkölaitteet ovat kytkettynä tietoliikenneverkkoihin. Tällaisten esineiden-Internet-verkon (IoT, Internet of Things) laitteiden avulla saamme kerättyä jatkossa yhä enemmän tietoa sellaisista toiminnoista, joista se ei ole ollut aikaisemmin mahdollista tai taloudellisesti kannattavaa. Näiden IoT-laitteiden osalta keskeisenä uhkana pidetään niiden tietoturvallisuuden toteuttamista.

2 Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelma

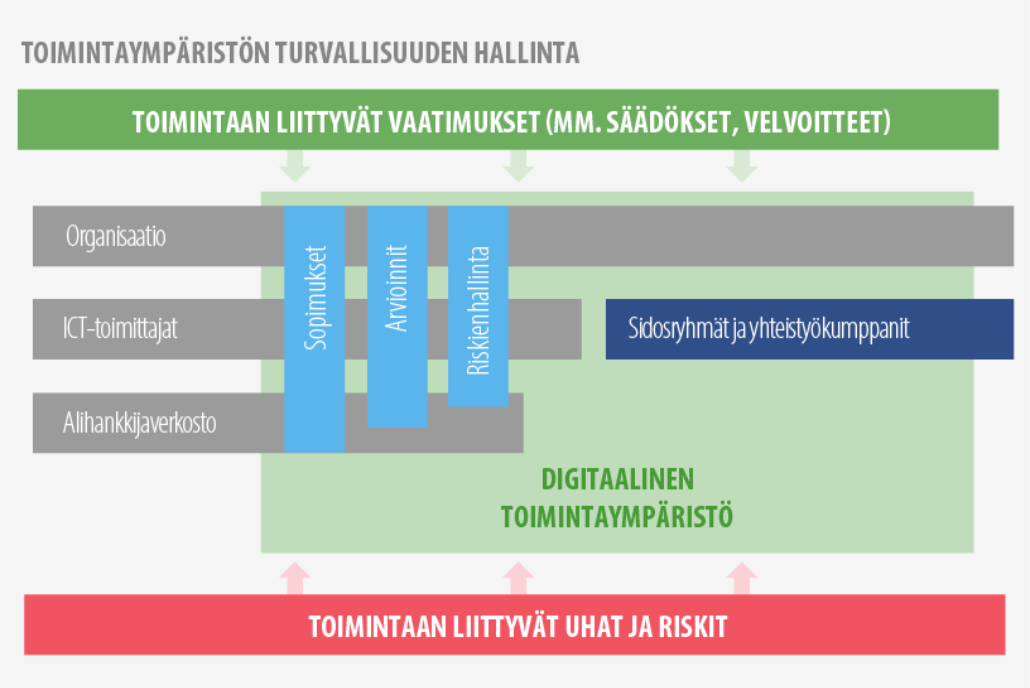
2.1 Ohjelman lähtökohdat

Julkisen hallinnon kehittämisohjelman laatimisesta on vastannut VAHTI-johtoryhmän jäsenistä sekä VAHTI-asiantuntijajaoston alaisuudessa toimivien viiden asiantuntijaryhmän puheenjohtajistosta koostuva ryhmä. Lisäksi tässä on huomioitu VAHTI-johtoryhmän ja sen alaisen asiantuntijajaoston jäsenten antamat kommentit kehittämisohjelman laatimisen eri vaiheissa sekä lausuntopalvelussa toteutetun lausuntokierroksen avulla saatu palaute.

Kehittämisohjelma on laadittu ottaen huomioon muun muassa seuraavat kokonaisuuteen vaikuttavat tekijät:

- Valtiovarainministeriön toteuttamat digitaalisen turvallisuuden kyselyt ja barometrit sekä näistä tehdyt havainnot sekä kehittämistoimenpide-ehdotukset
- Julkisen hallinnon digitaalisen turvallisuuden kokonaiskuva-raportoinnin kautta havaitut kehittämiskohteet
- Säädökset, muu regulaatio sekä laaditut selvitykset ja tarkastuskertomukset koskien digitaalisen turvallisuuden osa-alueita
- Toimintaympäristössä tapahtuvat tähän kokonaisuuteen liittyvät muutokset, tähän tehty kysely VAHTI-toimintaan osallistuville henkilöille
- Digitaalisen turvallisuuden tulevaisuuden ennakointi sen eri osa-alueiden näkökulmasta
- Kansainvälinen kehitys

Toimintaympäristöjen ja palveluiden muutokset edellyttävät myös riskienhallinnan jatkuvaa kehittämistä. Esimerkiksi yhteiskäyttöiset, globaalit pilvipalvelut, keinoälyn ja automatisaation hyödyntäminen luovat valtavia mahdollisuuksia, mutta samalla tuovat uusia uhkia, jotka pitää tunnistaa ja ottaa hallintaan.



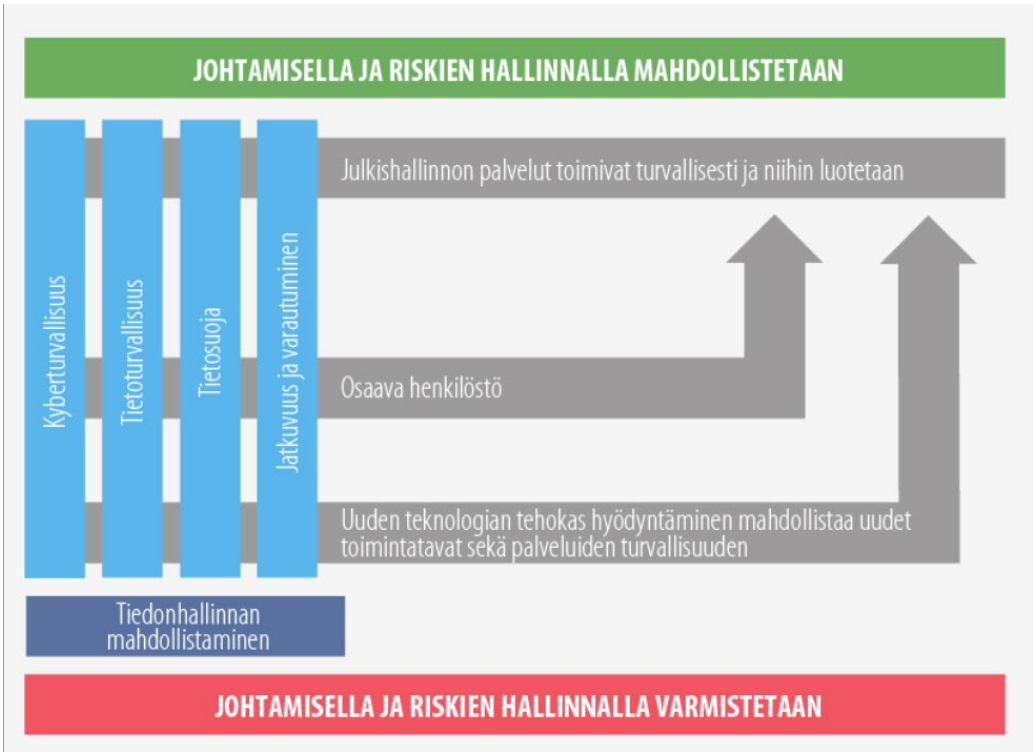
Kuva 3. Organisaation tulee varmistaa toimintaympäristön turvallisuus, jossa keskeisessä roolissa on palveluiden hankinta ja kilpailuttaminen tai oma kehittäminen, missä yhteydessä sovitaan myös turvallisuuden toteutumisen vaatimuksista.

Palveluiden tuottamisessa tulee huolehtia myös siihen liittyvän tietoturva-arkkitehtuurin huomioimisesta, joka mahdollistaa kustannustehokkaiden, yhteensopivien turvallisten palveluiden tuottamisen, joka on myös edellytys organisaatioiden väliselle tietojenvaihdolle.

2.2 Ohjelman tavoitteena varmistaa toimivat ja luotettavat digitaaliset palvelut

Kehittämisohjelman tavoitteena on varmistaa, että julkishallinnon digitaaliset palvelut toimivat ja että niihin luotetaan. Digitaalisten palveluiden tuottamisessa on tapahtunut merkittävä muutos viimeisen kymmenen vuoden aikana. Palvelutuotantoon liittyy usein eri palvelutoimittajia ja asiakkaita. Palvelut voivat olla riippuvaisia toisistaan ja niitä tuotetaan verkostomaisesti. Tietoja ja palveluja hyödynnetään eri tarpeisiin. Verkostomainen toiminta mahdollistaa entistä skaalautuvammat, kustannustehokkaat ja joustavammat digitaaliset palvelut. Tämä muutos on edellyttää myös jatkuvaa turvallisuuden johtamisen ja hallinnan kehittämistä.

Tällä kehittämisohjelmalla tuetaan ja mahdollistetaan digitalisaation toteuttaminen turvallisesti julkishallinnon palveluissa ja muussa sen toiminnassa. Tämä vahvistaa samalla palveluiden käyttäjien, niin kansalaisten, julkisen hallinnon henkilöstön, yritysten kuin muiden sidosryhmien luottamusta käytettäviin palveluihin ja toimintaan. Tämä tapahtuu kehittämisohjelmassa valittujen osa-alueiden avulla.



Kuva 4. Kehittämisohjelman keskeiset osa-alueet liittyvät johtamiseen ja riskienhallintaan, osaavaan henkilöstöön sekä uuden teknologian tehokkaaseen hyödyntämiseen palveluiden ja turvallisuuden toteuttamisessa.

Rakentamalla turvallisia palveluita, käsittelemällä palveluissa olevia tietoja vaatimustenmukaisesti sekä huolehtimalla myös häiriötilanteissa tarvittavasta viestinnästä saavutetaan asiakkaiden, kansalaisten ja muiden sidosryhmien luottamus. Tämä on samalla edellytys myös uuden teknologian käyttöönottamiselle palveluiden kehittämisessä.

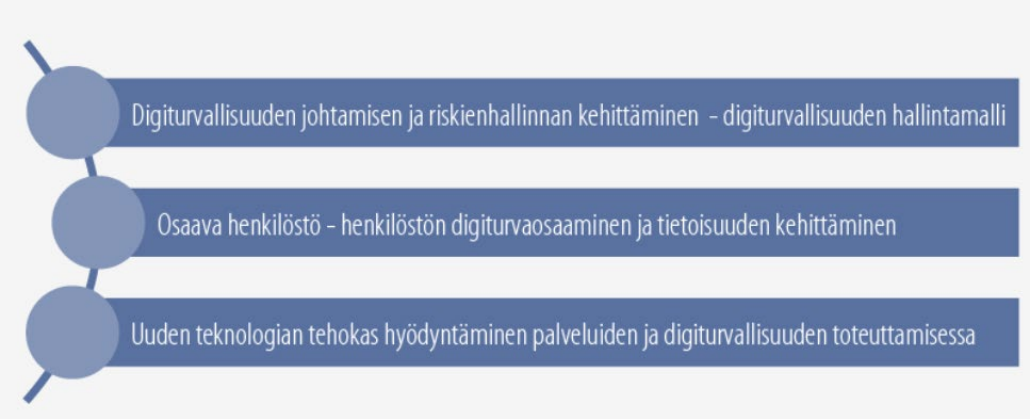
2.3 Kehittämisohjelman kattavuus

Kehittämisohjelma on tarkoitettu kattamaan koko julkinen hallinto. Kehittämisohjelman osa-alueet vaikuttavat välillisesti myös julkiselle hallinnolle palveluita tuottavien alihankkijoiden ja muiden sidosryhmien tuottamien palveluiden parantumiseen.

Kuva 5. Kehittämisohjelma on tarkoitettu julkisen hallinnon organisaatioille.

2.4 Kehittämisohjelman painoalueet

Valtiovarainministeriö on ottanut huomioon painoalueita valitessaan toimintaympäristöön liittyvät muutostekijät (liite 1) sekä kehittämisohjelmalle asetetut tavoitteet. Tavoitteiden saavuttamisen mahdollistamiseksi on valittu seuraavat kolme osa-aluetta, joita kehittämällä varmistetaan digitaalisen turvallisuuden laaja-alainen ja tarkoituksenmukainen kehittäminen julkisessa hallinnossa.



Kuva 6. Kehittämisohjelman kolme painoaluetta keskittyvät digitaalisen turvallisuuden keskeisin rakenteisiin, niin toimintaympäristön turvallisuuden johtamisen ja riskienhallinnan, henkilöstön kuin teknologian näkökulmasta. Painoalueiden kehittämistä tuetaan toimenpide-ohjelmalla.

2.4.1 Digiturvallisuuden johtamisen ja riskienhallinnan kehittäminen

Digitaalisen turvallisuuden johtamisen kehittäminen on valittu yhdeksi kehittämisen osa-alueeksi sen takia, että mitä nopeammin ja kattavammin uutta teknologiaa sekä uusia palveluita otetaan käyttöön, sitä enemmän se edellyttää digitaalisen turvallisuuden sovittamista osaksi organisaation toimintaan, etenkin johtamisen näkökulmasta. Samalla tämä varmistaa myös olemassa olevien palveluiden ja toiminnan turvaamisen. Organisaation käyttöönottamissa digitaalisissa palveluissa ja niiden tuotantotavoissa sekä alihankintaverkostoissa tapahtuu muutoksia kiihtyvällä vauhdilla. Tämän tulee heijastua myös organisaation johdon toimintaan turvallisuuden johtamisen kehittämisen näkökulmasta.

Menestyminen eri toiminnoissa ja tavoitteiden saavuttaminen on yhä enemmän riippuvainen onnistumisesta digitaalisten palveluiden ja prosessien kehittämisessä ja tuottamisessa. Organisaation johdon tulisi kyetä johtamaan tätä uudelleen muotoutuvaa kokonaisuutta nykyistä paremmin. Digitaalinen turvallisuus on yksi keskeinen osa alue ja sen merkitys on kasvamassa, joka edellyttää myös kokonaisvaltaisempaa digijohtamisen kehittämistä. Osana tätä tulee nykyistä paremmin ymmärtää, määrittää ja asettaa tarvittavien palveluratkaisuiden tietojen käytettävyydeltä ja turvallisuudelta edellytettävät vaatimukset.

Johtamisen, kuten digiturvallisuuden keskeisenä työkaluna toimii **riskienhallinta**. Organisaatio pystyy kehittämään omaa toimintaa tehokkaammin ja kustannustehokkaammin, kun sillä on toimiva riskienhallintaprosessi osana sen toimintaa, jossa on määritetty ne raamit, jonka sisällä se pystyy ottamaan riskejä (riskinottokyky) ja myös niitä käytännössä ottaa (riskinottohalukkuus). Osa toimivaa riskienhallintaa on kyky käsitellä ja hyväksyä sekä hallita jäännösriskejä; nykyaikana ei ole mahdollista toimia ilman jäännösriskiä.

Digitaalisen turvallisuuden johtaminen edellyttää

- riskilähtöistä toimintamallia organisaation ja digitaalisen turvallisuuden johtamisessa - riskienhallinta varmistaa, mutta myös mahdollistaa organisaation tavoitteiden saavuttamisen, jatkuvan toiminnan sekä toiminnan kehittymisen esimerkiksi uudenlaisten, turvallisten digitaalisten palveluiden avulla

- turvallisuuden eri osa-alueiden ymmärtämistä ja niiden tärkeyden tunnistamista osana organisaation toimintaa sekä koko toimintaverkostossa

- arkkitehtuurien hyödyntämistä yhteentoimivuuden ja tietojen sujuvan jakamisen mahdollistamiseksi

- toimintaverkoston hallintaa; sopimuksissa ja vaatimuksissa kuvattujen velvoitteiden seuranta osana sekä tarvittavien arviointien toteuttaminen

- vastuiden kuvaamista ja määrittämistä niin organisaation sisällä kuin sen keskeisten toimittajien ja sidosryhmien kesken

- tarvittavia resursseja käytännön tasolla toteuttaa digitaalisen turvallisuuden eri osa-alueilta edellytettäviä vaatimuksia

- kokonaisuuden raportointia ja seurantaa johdon tasolla, mutta myös organisaatiolle tuottavien alihankkijoiden osalta

Osana tämän kehittämisohjelman toimenpideohjelmaa luodaan johtamisen ja riskienhallinnan tueksi uusia toimintamalleja sekä toteutetaan yhteishanke julkisen hallinnon organisaatioille tämän osa-alueen kehittämiseksi.

Niiltä osin kuin organisaatiolla on jo olemassa olevat laadukkaat riskienhallinnan käytännöt ja järjestelmät, voivat organisaatiot hyödyntää niitä huomioiden kehittämisohjelmasta saatavilla olevat muut parannukset.

Kuva 7. Riskienhallinnan tulee olla dynaamista ja huomioida toiminnan luonne, kriittisyys sekä toimintaympäristön muutokset. Organisaation johdon tehtävä on asettaa puitteet riskienhallinnan toteuttamiselle sekä huolehtia kokonaisuuden toiminnasta. Riskinottokyky ja halu pitää vaihdella arvioitavan toiminnon / kohteen mukaisesti, mitä suurempi mahdollinen vahinko on kyseessä, sitä tärkeämpää on kiinnittää huomiota riskienhallinnan toimivuuteen ja tunnistettujen riskien hallintaan.

Organisaation johto on vastuussa, että se on liittänyt digitaalisen turvallisuuden johtamisen ja sen vaatiman osaamisen osaksi sen johtamisjärjestelmää.

Kuva 8. Organisaation johdon vastuuna on huolehtia digitaalisen turvallisuuden toteutumisesta sen toiminnassa sekä omassa organisaatiossa, että sille tuotettujen palveluiden ja toimintojen osalta. Organisaatiossa tulee olla vastuutettu ja nimetty keskeiset digiturvallisuuden roolit, esimerkiksi tietoturvallisuuden ja tietosuojan osalta.

Käytännössä tämä tapahtuu kokonaisuuden vastuuhenkilöiden toteuttamana siten, että kokonaisuutta varten luodaan digitaalisen turvallisuuden johtamisen ja hallinnan malli, jonka avulla organisaatio varmistaa vaatimustenmukaisuuden toteutumisen sen toiminnassa. Kuten kaikessa toiminnassa, myös digitaalisessa turvallisuudessa henkilöstön rooli on keskeinen, minkä johdosta henkilöstön osaamisen kehittäminen on yksi tämän kehittämisohjelman painoalueita. Organisaation tulee huolehtia myös sen ydin/liiketoiminnan kehittämiseen osallistuvan toimittajaverkoston osaamisesta ja turvallisuustietoisuudesta, ja osallistua sen asiantuntijoiden kouluttamiseen.

Valtionhallinnossa osana toimenpide-ohjelman toteuttamista tulee varmistaa, miten tätä kehittämisohjelmaa voidaan toteuttaa tehokkaasti esimerkiksi valtioneuvostossa ja ministeriöiden hallinnonaloilla.

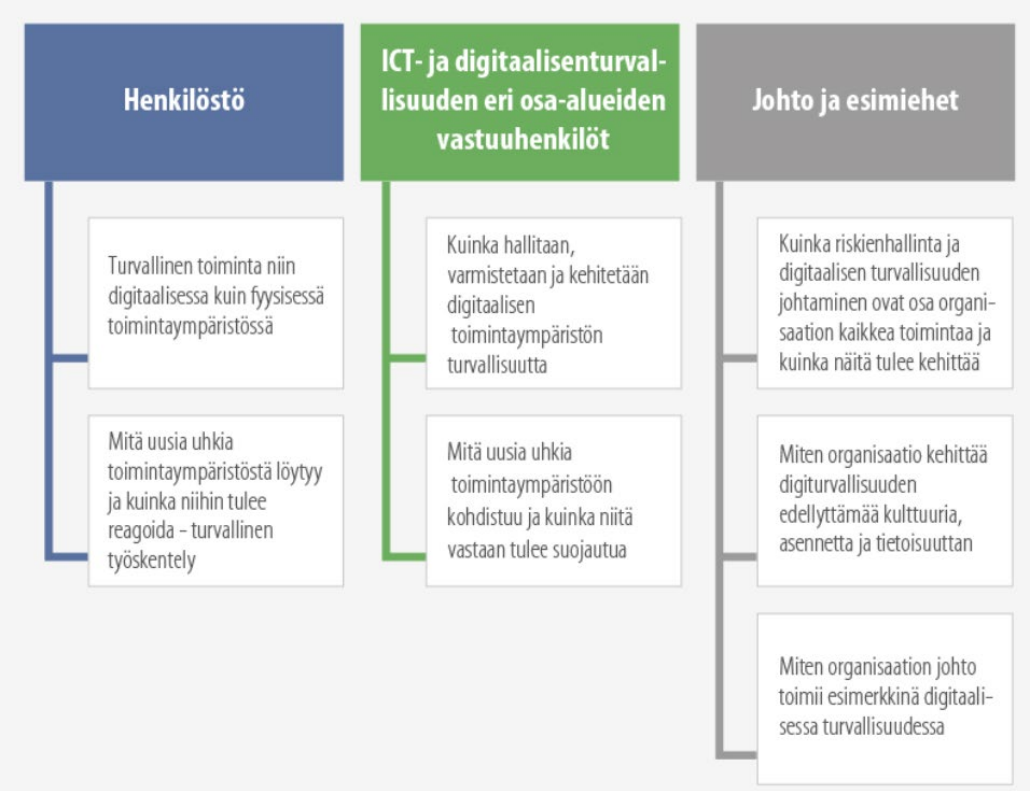
2.4.2 Osaava henkilöstö - henkilöstön digiturvaosaaminen ja tietoisuuden kehittäminen

Tässä kehittämisohjelmassa on aikaisemmin nostettu esille henkilöstön keskeinen, kriittinen rooli digitaalisen turvallisuuden toteuttamisessa organisaatiossa. Tämän kehittämisalueen avulla varmistamme, että julkisen hallinnon henkilöstö toimii jatkossa entistä turvallisemmin nopeasti muuttuvassa digitaalisessa toimintaympäristössä.

Tämä edellyttää uudenlaista digitaalisen turvallisuuden eri osa-alueiden koulutuksen kehittämistä ja toteuttamista. Kertaluonteinen tai vuosittainen koulutus ei enää riitä; digitaalisessa toimintaympäristössä tapahtuvat julkista hallintoa kohtaavat uhkakuvat kehittyvät entistä nopeammin. Tämän johdosta tarvitaan säännöllistä, paremmin toimintaympäristön muutokset ja nopeasti kehittyvät uhkakuvat huomioivaa koulutusta ja aktiivista viestintää. Tämän toteuttaminen tarvittavalla tasolla esimerkiksi pienissä organisaatioissa ei ole mahdollista ja taloudellista, joten se tulee jatkossa tapahtua keskitetysti.

Valtiovarainministeriön valmistelema tiedonhallintalaki vaikuttaa astuessaan voimaan merkittävästi julkisen hallinnon digitaaliseen turvallisuuteen, joka tulee ottaa huomioon henkilöstön koulutuksessa ja ohjeistuksessa. Laki sinällään ei vaikuta tai muuta tämän kokonaisuuden henkilöstön ohjeistamiseen ja koulutukseen liittyviä perusperiaatteita, ainoastaan tarkentaa niitä esimerkiksi tietoaineistojen luokittelun osalta.

Jatkossa tarvitaan paremmin sovitettua ja suunnattua koulutusta ja viestintää hyödyntäen uuden teknologian tarjoamia mahdollisuuksia, esimerkiksi seuraaville kohderyhmille käsitellen alla mainittuja osa-alueita:



Kuva 9. Osaamista tulee kehittää keskitetysti eri kohderyhmille varmistaen koulutuksen ja tiedottamisen laadun, säännöllisyyden ja kustannustehokkuuden.

Osa koulutuksesta tulee toteuttaa siten, että julkisen hallinnon henkilöstön osalta tulee asettaa koulutuksien ja niihin liittyvien testien suorittaminen pakolliseksi, esimerkiksi osaksi palveluissa edellytettävien käyttöoikeuksien saamista.

Perinteisten koulutusten rinnalle tulee luoda uudenlaisia malleja osaamisen ja uhkatietoisuuden parantamiseksi hyödyntäen esimerkiksi pelillistämisen tarjoamia mahdollisuuksia.

Koska usealla julkisen hallinnon organisaatiolla on jo käytössä omia koulutusjärjestelmiä, voivat ne hyödyntää niissä yhteisesti kaikille luotavia materiaaleja.

2.4.3 Uuden teknologian tehokas hyödyntäminen palveluiden ja digiturvallisuuden toteuttamisessa

Valtiovarainministeriön keräämä kokonaiskuva osoittaa ja ennustaa, että tulemme jatkossa kokemaan yhä useammin erilaisia ICT-palvelutuotantoon liittyviä häiriöitä, tieto- ja kyberturvallisuuteen sekä tietosuojaan liittyviä poikkeamia Suomi etenee julkisen hallinnon digitalisoinnoin osalta globaalisti kärkijoukoissa, jolloin myös edelläkävijät joutuvat kokemaan ensimmäisten joukossa siihen liittyviä uhkia. Täten uuden teknologian käyttöönottoon liittyy uhkia, mutta ennen kaikkea valtavia mahdollisuuksia, jossa Suomi on toistaiseksi menestynyt loistavasti.

Julkiselle hallinnolle tuotettavien palveluiden yhteyteen tulee kasvattaa nykyistä tehokkaampaa havainnointikykyä ja sen mukaista reagointia meidän toimintaa uhkaavien riskien osalta. Uhkakuvien kasvaessa mahdollisesti tulevaisuudessa eksponentiaalisesti, tämä edellyttää sekä keinoälypohjaisen että sen tuottaman tiedon asiantuntijavoimin tapahtuvan analysointikyvyn kehittämistä. Kuten useissa muissa tässä kehittämisohjelmassa esille nostetuissa kohteissa, tätä tulisi keskittää toiminnan laadun, tiedonvälityksen, yhteistyön sekä kustannustehokkuuden varmistamiseksi.

Kaikista tässä kehittämisohjelmassa esitettävistä toimenpiteistä huolimatta tulemme kokemaan jatkossa yhä enemmän toimintaamme kohdistuvia uhkia. Tämä johtuu siitä, että tietoverkko- ja kyberrikollisuus tulee entisestään laajentumaan ja globalisoitumaan.

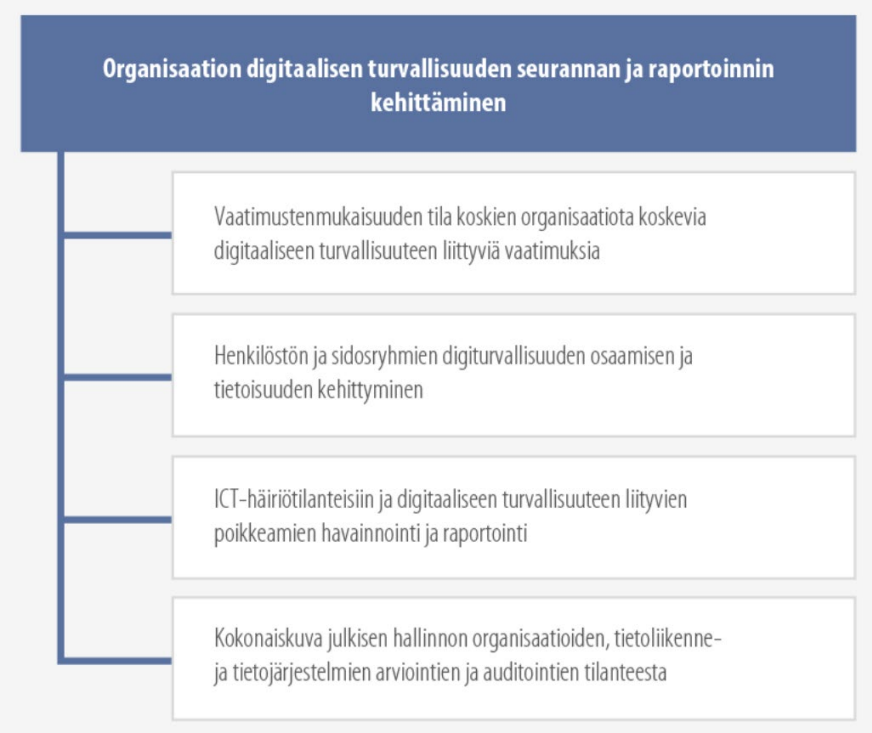
Eräs syy tähän on se, että internet-verkko ja digitaaliset palvelut eivät ole vielä kaikkialla maailmassa läheskään samalla tasolla kuin pitempään näitä hyödyntäneissä, teknologiaan ja uusiin palveluihin panostaneissa valtioissa. Tällöin nämä nopeasti kehittyvät markkinat houkuttelevat rikollisia entisestään kehittämään keinoja taloudellisen edun saavuttamiseksi uusien käyttäjien ja digitaalisten palveluiden avulla. Tästä kehityksestä myös Suomi saa osansa, vaikka emme välttämättä ole tällaisen toiminnan aktiivinen kohde, mutta globaalin tietoverkko- ja kyberrikollisuuden kehittyminen heijastuu myös tällä tavalla Suomalaiseen yhteiskuntaan. Se, että Suomi on maailman johtavia maita uuden teknologian käyttöönottamisessa, altistaa meidät myös ensimmäisten joukossa siihen kohdistuville uhille. Me emme voi vaikuttaa suoraan siihen, kuinka paljon meitä vastaan hyökätään, mutta me voimme vaikuttaa tällaisten hyökkäysten havaitsemiseen sekä reagointikykyyn ja sitä kautta toiminnan palauttamiseen sen kriittisyydelle määritettyjen vaatimusten mukaisesti.

Edellä kuvatun toiminnan ohella toinen, ei tietoisesti meitä vastaan kohdistuva uhka liittyy ICT-palveluiden ja niiden tuottamiseen liittyviin häiriöihin. Uuden teknologian

käyttöönotto tulee tapahtumaan kiihtyvällä vauhdilla, joka aiheuttaa haasteita sen luotettavan ja turvallisen toiminnan testaamiseen. Julkisen hallinnon ICT-palveluiden keskittäminen kasvattaa laajavaikutteisten häiriöiden mahdollisuutta, aikaisemmin organisaation itse tuottaman palvelun häiriön vain organisaatiokohtainen vaikutus tulee laajentumaan jopa koko yhteiskunnan tasolle keskitetyn palvelutuotannon häiriintyessä. Tällöin myös tällaisten palveluiden palvelutuotannon häiriötilanteiden hallinnassa tulee hyödyntää uutta teknologiaa, esimerkiksi automatisaatiota ja keinoälyä.

Tässä kehittämisohjelman kolmannessa osa-alueessa kehitetään organisaation omia digitaalista turvallisuutta kehittäviä toimintoja seurannan ja raportoinnin näkökulmasta. Kun organisaatio pystyy paremmin tunnistamaan sen oman digitaalisen turvallisuuden toiminnan tason, sen avulla organisaatio pystyy myös paremmin kehittämään omaa turvallisuutta muodostettavan kokonaiskuvan avulla. Vastaavasti valtiovarainministeriö pystyy tämän avulla muodostamaan koko julkisen hallinnon digitaalisen turvallisuuden kokonaiskuvan ja sen avulla vaikuttamaan esimerkiksi tunnistettujen erityistä tukea tai toimenpiteitä tarvitsevien osa-alueiden kehittämiseen.

Keskeisiä, toimenpideohjelmassa kehitettäviä osa-alueita ovat esimerkiksi:



Kuva 10. Digiturvallisuudessa tulee huolehtia laajasti turvallisuuden eri osa-alueiden kehittämisestä. Jokaisen organisaation tulisi entistä paremmin pystyä havainnoimaan, seuraamaan ja mittamaan oman organisaation digitaalisen turvallisuuden tilannetta.

2.5 Kokonaisarkkitehtuurin toteuttamisella edistetään turvallista digitalisaatiota

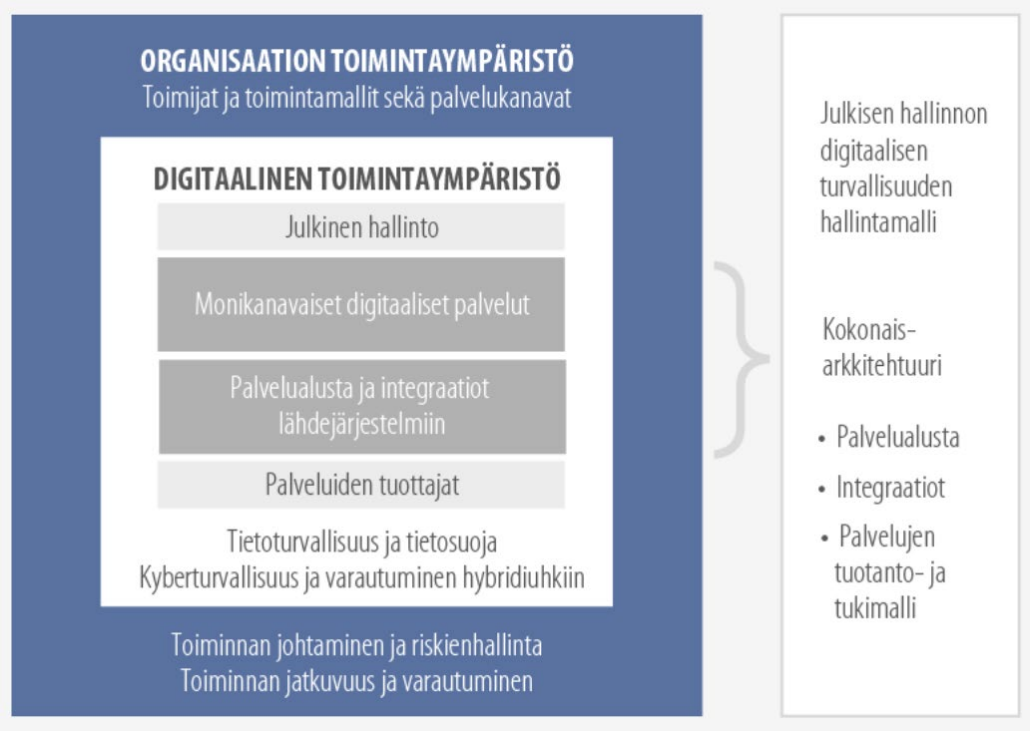
Yhteiskunnassa tapahtuva toimintatapojen muutos digitalisoimalla julkisen hallinnon palveluita edellyttää uudella tavalla digiturvallisuuden johtamista ja toteuttamista. Tällä myös mahdollistetaan, että julkisen hallinnon toimintatavat ja digitaaliset palvelut ovat tehokkaita sekä yhteensopivia vastaten asiakkaiden tarpeisiin.

Kuva 11. Kuvassa keskeisiä julkisten palveluiden digitalisoimisessa huomioitavia osa-alueita, jotka yhdessä ovat osa digitalisaation hallintamallia.

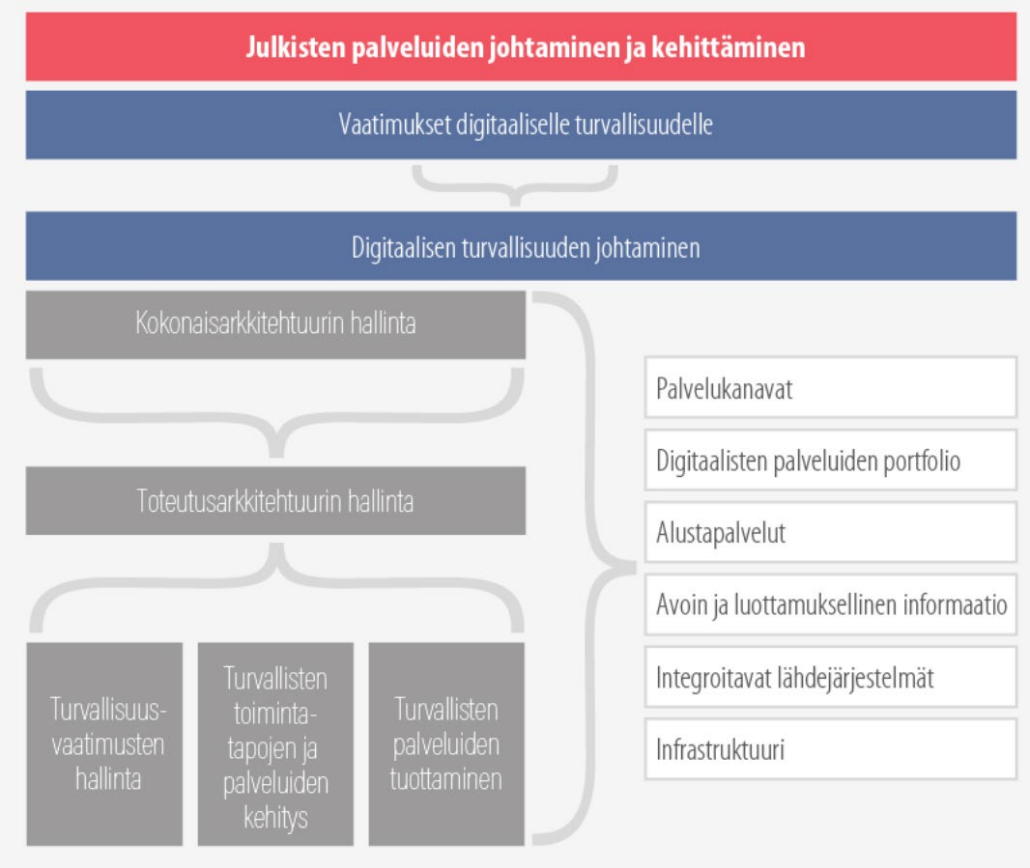
Tässä keskeinen rooli on kokonaisarkkitehtuurilla, joka mahdollistaa uusien työtapojen kytkeytymisen niitä tukeviin digitaalisiin palveluihin. Digitaalisten palveluiden kehittäminen edellyttää puolestaan modernia palveluympäristöä, joka hyödyntää yhteiskäyttöisiä tietoja turvallisesti sekä liittää järjestelmät ja infrastruktuurit hallituiksi kokonaisuuksiksi.

Julkisten palveluiden turvallinen digitalisaatio on henkisten ja taloudellisten resurssien, toimintatapojen sekä -rakenteiden muutosta. Turvallinen digitalisaatio parantaa toimintaa ja luo mahdollisuuksia esimerkiksi erilaisille ekosysteemeille.

Tiedon jakaminen ja yhteiskäyttö ovat toimivan moniviranomaisyhteistyön perusedellytys. Digitaalisen turvallisuuden kehittäminen tapahtuu aseittain osana nykyisten toimintatapojen ja palveluiden kehittämistä sekä uutena kehittämistyönä.



Kuva 12. Organisaation toimintaympäristön ja digitaalisen toimintaympäristön kehittämisessä tarvittavat rajapinnat sekä sovittaminen kokonaisarkkitehtuuriin ja tiettyihin digiturvallisuuden osa-alueisiin.

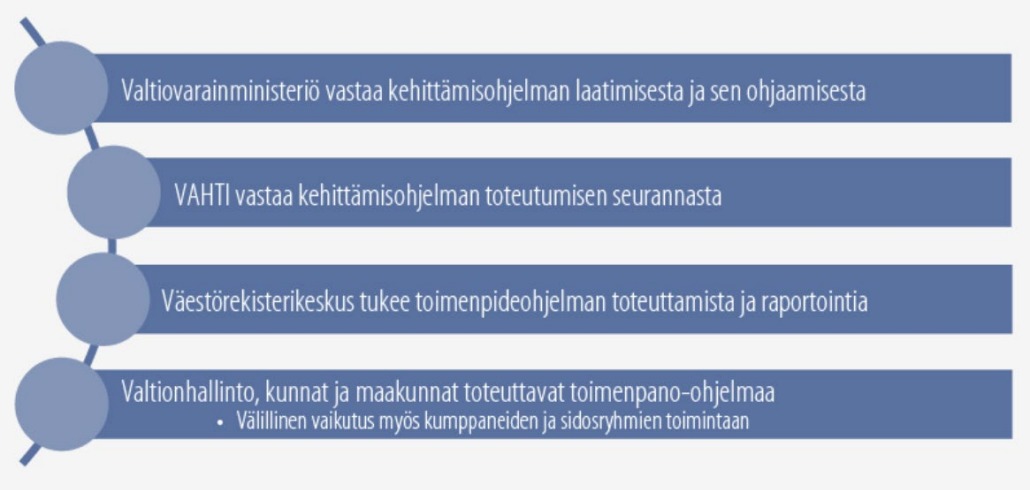


Kuva 13. Noudattamalla kokonaisarkkitehtuurimallia ja johtamalla siitä tekninen toteutusarkkitehtuuri luodaan tarvittava toteutusympäristö digitaalisille palveluille. Arkkitehtuurin avulla mm. ohjataan digitaalisten palveluiden kehittämistä ja palvelutuotantoa sekä varmistetaan myös digitaalisen turvallisuuden vaatimusten huomioiminen.

2.6 Kehittämisohjelman osapuolten vastuut

Kehittämisohjelman laatimisesta on vastannut valtiovarainministeriö ja se vastaa myös toimeenpano-ohjelman ohjaamisesta. Kehittämisohjelman ja toimeenpano-ohjelman toteutumisen seurannasta vastaa julkisen hallinnon digitaalisen turvallisuuden johtoryhmä. Väestörekisterikeskuksen vastuulla on kehittämisohjelman toimenpide-ohjelman toimenpiteiden tarjoaminen julkiselle hallinnolle ja raportointi toimenpiteiden etenemisestä valtiovarainministeriölle sekä VAHTIlle.

Valtionhallinto, kunnat ja maakunnat osallistuvat toimenpide-ohjelman toteuttamiseen kehittämisohjelmalle asetettujen tavoitteiden saavuttamiseksi.



Kuva 14. Kehittämisohjelman ja toimenpide-ohjelman vastuut.

2.7 Julkisen hallinnon digitaalisen turvallisuuden toimenpideohjelma

Tämän kehittämisohjelman tueksi on laadittu toimenpide-ohjelma vuosille 2018-2021. Valtaosa tässä kehittämisohjelmassa esille nostetuista tehtävistä ovat sellaisia, joita organisaation tulisi kehittää normaalisti osana turvallisuuden ylläpitoa ja kehittämistä. Toimeenpano-ohjelmalla halutaan priorisoida, osin keskittää ja yhteensovittaa kehittämistä koko julkisen hallinnon näkökulmasta.

Jokaiseen kehittämisohjelman keskeiseen kohtaan on luotu useampi toimenpide, joiden avulla kyseistä osa-aluetta voidaan kehittää sille asetettujen tavoitteiden saavuttamiseksi. Näistä toimenpiteistä on luotu kehittämisohjelman toimenpide-ohjelma. Sen ohjauksesta vastaa valtiovarainministeriö ja sen toteuttamisesta ja raportoinnista Väestörekisterikeskus. Toimeenpano-ohjelma kohdistetaan julkisen hallinnon organisaatioihin.

Kehittämistoimenpiteiden määrän sijaan priorisoidaan niiden laatua tunnistamalla sellaisia toimenpiteitä, joiden avulla voidaan laaja-alaisesti kehittää koko julkisen hallinnon digitaalista turvallisuutta kehittämisohjelman painotusten perusteella

Jokaiselle toimenpiteelle on

- luotu selkeä tavoite
- asetettu sen toimeenpanon toteuttamisesta vastaava projekti
- budjetti sen toteuttamiseksi
- vuosittaiset seurantamittarit
- seuranta ja raportointi toimenpiteiden etenemisestä

Toimeenpano-ohjelma kytketään soveltuvin osin tulevan tiedonhallintalain toimeenpanoon.

Toimenpideohjelma on myös erikseen julkaistava Liite 1. Tämä mahdollistaa myös sen, että toimenpideohjelmaan voidaan tuoda uusia toimenpiteitä kehittämisohjelman kuluessa osana valtiovarainministeriön vuosittaista kehittämisohjelman etenemisen tarkastelua.

3 Kehittämisohjelman vaikuttavuus ja mittarit

Valtiovarainministeriö tulee seuraamaan ja arvioimaan kehittämisohjelman vaikuttavuutta mittareiden ja muun seurantatiedon avulla. Jokaiselle toimenpiteelle luodaan omat mittarit, mutta myös kokonaisuutta seurataan sitä varten luotavien mittareiden avulla

Valtiovarainministeriö luo uuden digiturvallisuuden mittariston osana tätä julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelmaa, jossa mitataan kattavasti digiturvallisuuden kaikkien osa-alueiden kehittymistä julkisessa hallinnossa. Samassa yhteydessä kehitetään digiturvallisuuden strategisen kokonaiskuvan keräämistä siten, että organisaatiot saavat käyttöönsä niiden oman toiminnan kehittämisen ja toiminnan seurantaan tarkoitetun mallin. Tämän avulla organisaatio voi itse varmistua sen digiturvallisuuden eri osa-alueiden tilanteesta ja kehittymisestä organisaation toiminnalle asetettujen vaatimusten mukaisesti.

Näillä tuetaan samalla organisaatioiden digiturvallisuuden johtamista ja tämä toimii myös osana digiturvallisuuden hallintamallia. Näiden kehittäminen tapahtuu osana toimenpiteitä yksi ja neljä.

Liite 1. Julkisen hallinnon digitaalisen turvallisuuden toimenpideohjelma vuosille 2018-2021

Tässä liitteessä on kuvattu 5 toimenpidettä, joiden avulla kehittämisohjelman kolmea painoaluetta edistetään. Jokaisesta toimenpiteestä tuotetaan yksityiskohtainen projektisuunnitelma. Valtiovarainministeriö arvioi vuosittain tarpeen uusien toimenpiteiden käynnistämiseksi. Nämä toimenpiteet ovat samalla osa valtiovarainministeriön toteuttamia Suomen kyberturvallisuusstrategian toimeenpanoa edistäviä hankkeita.

Toimenpide 1 Digitaalisen turvallisuuden johtamisen ja riskienhallinnan kehittäminen

Kohderyhmä:	Organisaation johto sekä ICT- ja tietoturvallisuudesta sekä tietosuojasta vastaavat asiantuntijat, arkkitehdit. Organisaation ylimmän johdon vastuuhenkilö sekä muut asiantuntijat osallistuvat koulutuksiin ja yhteishankkeeseen.
Tavoite:	Projektin avulla organisaatio saa varmistettua, että sillä on tarvittava osaaminen digitaalisen turvallisuuden johtamiseksi, kehittämiseksi ja hallitsemiseksi muuttuvassa toimintaympäristössä. Tässä hyödynnetään tätä varten luotua digiturvariskien hallintamallia. Yhteishankkeessa jalkautetaan luotu JHKA 2.0- pohjainen arkkitehtuurin kuvausmalli.
Aikataulu:	1/2019 – 12/2021
Toteutusvastuu:	VRK rakentaa ohjelman yhdessä käyttäen VAHTI-asiantuntijajaostoa sekä VAHTI-toiminnassa olevien organisaatioiden asiantuntemusta hyödyntäen
Mittari:	Osallistuvien organisaatioiden määrä (osa-alueen kattavuus) Osallistuneiden organisaation tyytyväisyys projektiin Mittarit digiturvallisuuden johtamisen toteutumisen osalta ennen ja jälkeen yhteishankkeen Mittarit digiturvariskien hallinnan toteutumisen osalta ennen ja jälkeen yhteishankkeen
Muuta:	Osana koulutusta toteutetaan myös riskienhallinnan kehittämiseen liittyvät toimenpiteet ja osaamisen kehittäminen, jota esimerkiksi tiedonhallintalaki tulee edellyttämään.

Toimenpide 2 Digitaalisen turvallisuuden soveltamis- ja arviointikehikon toteuttaminen

Kohderyhmä: ICT- ja turvallisuuden vastuuhenkilöt

Tavoite:

Valtionhallinnossa voimassa olevat tietoturvallisuutta koskevat ohjeet pohjautuvat vuonna 2010 voimaan astuneeseen tietoturvallisuusasetukseen. Nyt tämä malli korvataan uudella digitaalisen turvallisuuden soveltamis- ja arviointikehikolla, joka samalla tukee ja toimii sekä tiedonhallintalain toimeenpanoa edistävänä hankkeena, että kehittää julkisen hallinnon digitaalisen turvallisuuden johtamista ja käytännön tason toteuttamista.

Projektissa toteutetaan uusi lainsäädäntöä tukeva digitaalisen turvallisuuden soveltamiskehikko, jossa kuvataan hyviä käytäntöjä lainsäädännön sisältämien vaatimusten toteuttamiseksi julkisessa hallinnossa. sekä tarvittavat arviointikriteerit eri osa-alueiden (organisaatio, ICT-palvelukokonaisuus, hankinnat) vaatimustenmukaisuuden arvioimiseksi. Arviointi, samoin kuin vaatimukset, voi kohdistua esimerkiksi organisaatioon, tietoliikenne- tai tietojärjestelmään, hankintaan. Samassa yhteydessä luodaan prosessit vaatimustenmukaisuuden raportoimiseksi osaksi organisaation digitaalisen turvallisuuden kokonaiskuvan toteuttamista. Tällä korvataan aikaisemmin erikseen toteutetut VAHTI-organisaatiokyselyt.

Aikataulu: 1/2019 – 12/2021

Toteutusvastuu: VRK toteuttaa soveltamis- ja arviointikehikon yhdessä keskeisten yhteistyötahojen kanssa ja pilotoi sitä eri kokoisten kohderyhmien kanssa ennen sen toteuttamista.

Mittari: Soveltamis- ja arviointikehikon käyttöönottaneiden organisaatioiden määrä (kattavuus)
Osallistuneiden organisaation tyytyväisyys projektiin

Muuta:

Soveltamis- ja arviointikehikon jalkauttaminen toteutetaan yhteishankkeiden avulla. Yhteishankkeet pohjautuvat niitä varten luotuun ohjeistukseen, jonka avulla organisaatio saa käyttöönsä digiturvallisuuden hallintajärjestelmämallin. Hallintajärjestelmästä luodaan esimerkiksi kaksi mallia, vähimmäistason malli,
joka on tarkoitettu ja soveltuu pienemmille organisaatioille sekä kehittyneempi malli, joka on tarkoitettu sellaisille organisaatioille, joiden turvallisuuden hallinta edellyttää kehittyneempää hallintamallia.

Toimenpide 3 Julkisen hallinnon digitaalisen turvallisuuden koulutusjärjestelmä sekä digiturvasovellus

Kohderyhmä: Kolme eri kohderyhmää; julkisen hallinnon henkilöstö, ICT-, tietoturva ja tietosuojahenkilöstö sekä johto ja esimiehet, osa kehitettävistä palveluista voidaan mahdollisesti tuotteistaa tarjottavaksi myös kansalaisille sekä julkiseen hallintoon tuottavien yritysten henkilöstölle.

Tavoite: Julkisen hallinnon organisaatioiden käytössä on keskitetty digitaalisen turvallisuuden koulutusjärjestelmä. Organisaation henkilöstö osallistuu sille tarkoitettuihin velvoittaviin koulutuksiin ja ajankohtaiskatsauksiin.

Koulutusten läpikäynti ja osallistuminen ajankohtaiskatsauksiin on edellytys käyttöoikeuksien saamiselle ja säilyttämiselle organisaatiossa.

Julkisen hallinnon organisaatioille ja henkilöstöllä on käytössä digiturvasovellus, joka mahdollistaa henkilöstön tiedottamisen ja koulutuksen digiturvan eri osa-alueilta.

Aikataulu: 1/2019 – 12/2021

Toteutusvastuu: VRK toteuttaa koulutusjärjestelmän yhdessä eOppivan ja Valtorin kanssa varmistaen, että palvelu on käytettävissä koko julkisessa hallinnossa. Digiturvasovellus toteutetaan käyttäen VRK:n käytössä olevia sovelluskehitysmalleja.

Mittari: Osallistuvien organisaatioiden määrä (kattavuus julkisesta hallinnosta)
Koulutukseen osallistuneiden henkilöiden määrä (kattavuus)
Koulutusten läpäisyprosentti
Digiturvasovelluksen latausmäärä ja käytön yleistyminen sekä palaute
Osallistuneiden organisaation tyytyväisyys projektiin

Muuta: Organisaatio voi saada vastaavat materiaalit käyttöön omaan koulutusjärjestelmään. Osaksi kokonaisuutta toteutetaan myös digitaalisen turvallisuuden työkalupakki, joka sisältää materiaalipankin sekä muita sellaisia työkaluja, ohjeita ja materiaaleja, joita organisaatio voi hyödyntää oman toiminnan kehittämisessä. Materiaalipankin materiaalit julkaistaan avoimena datana.

Toimenpide 4 Julkisen hallinnon digitaalisen turvallisuuden kokonaiskuvan raportoinnin kehittäminen

Kohderyhmä: Julkisen hallinnon organisaatiot, niiden johto, tietohallinto ja turvallisuuden vastuuhenkilöt

Tavoite: Projektin avulla digitalisoidaan ja uudistetaan nykyaikaisen digiturvallisuuden kehittämisessä tarvittavien mittareiden kerääminen ja julkaiseminen. Projektin avulla siirrytään perinteisestä, kertaluonteisesti vuosittain toteutetuista kyselyistä ja raportoinneista ajantasaisesti tehtäviin sähköistä palvelua käyttävään raportointialustaan.

Aikataulu: 1/2019 – 12/2021

Toteutusvastuu: VRK vastaa palvelun suunnittelusta ja toteuttamisesta.

Mittari: Kokonaiskuvaan kuuluvien mittareiden lukumäärä
Palvelun käyttöönottaneiden organisaatioiden lukumäärä (kattavuus)
Osallistuneiden organisaation tyytyväisyys projektiin ja sen itsensä saamaan kokonaiskuvaan palvelun avulla

Muuta:

Tämän hankkeen tarkoituksena on digitalisoida yksittäiset kyselyt ja toiminnot yhtenäiseksi, ajantasaiseksi palveluksi, jonka avulla julkisen hallinnon organisaatioista saadaan selville esimerkiksi:

- organisaation ja tietojärjestelmien vaatimustenmukaisuuden tila verrattuna uusiin, ns. VAHTI -100 soveltamis/arviointikehikon mukanaan tuomiin malleihin (vaatimustenmukaisuuden tila)
- henkilöstön ja johdon asenne ja toimintakulttuurin tila ei kertaluonteisesti vaan siten, että henkilöstö voi vastata tähän periaatteessa jatkuvasti sen hetkisen tilanteen ja tunteen mukaisesti (happy or not –malli)
- Digitaalisen turvallisuuden osa-alueisiin liittyvät häiriöt ja poikkeamat sitä mukaa kun organisaatiossa niitä tapahtuu
- toteutetut tietoturva-arvioinnit ja auditoinnit metatietojen osalta
- itse toteutetut ja osallistuminen digitaalisen turvallisuuden harjoituksiin (osa tieto- ja kyberturvallisuusharjoitussuunnitelman seurantaa)

Toimenpide 5 Digitaalisen turvallisuuden harjoitusohjelma ja sen toteuttaminen v. 2018-2021

Kohderyhmä:	Julkisen hallinnon organisaatiot ja niiden alihankkijat ja mahdolliset sidosryhmät
Tavoite:	Valtiovarainministeriö vastaa julkisen hallinnon digitaalisen turvallisuuden harjoitusohjelman toteuttamisesta. Sen laatimisesta ja operatiivisesta toteuttamisesta vastaa Väestörekisterikeskus. Harjoitusohjelman avulla kuvataan julkisen hallinnon tarve sekä käytettävät menetelmät koskien digitaalista turvallisuutta edistävää harjoitustoimintaa. Harjoitusohjelmassa jossa kuvataan tarkemmin lähivuosien aikana toteutettavaksi tarkoitetut keskeiset harjoitukset sekä ylläpidetään tähän liittyvää harjoituskalenteria. Harjoitusohjelmaa aletaan toteuttaa vuonna 2019, jonka perusteella julkisen hallinnon organisaatiot voivat osallistua suunniteltaviin harjoituksiin. Harjoitusten avulla varmistetaan vuosittain harjoituksille asetettujen tavoitteiden saavuttaminen, kasvatetaan kyvykkyyttä selviytyä erilaisista organisaation digitaaliseen toimintaympäristöön liittyvistä häiriöistä ja loukkauksista.
Aikataulu:	1/2019 – 12/2021
Toteutusvastuu:	VRK toteuttaa harjoitusmallin yhteistyössä keskeisten sidosryhmien, esimerkiksi Huoltovarmuuskeskuksen, Puolustusvoimien, tietosuojavaltuutetun toimiston, Turvallisuuskomitean ja Viestintäviraston Kyberturvallisuuskeskuksen kanssa.
Mittari:	Toteutettujen harjoitusten määrä ja niiden laatu Harjoituksiin osallistuneiden organisaatioiden määrä (kattavuus) Osallistuneiden organisaation tyytyväisyys projektiin
Muuta:	-

Liite 2. Lähteet

OECD - Digitaaliseen turvallisuuteen kohdistuvien riskien hallinta taloudellisen ja yhteiskunnallisen hyvinvoinnin edistämiseksi

Linkki:
http://julkaisut.valtioneuvosto.fi/handle/10024/75412

Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä (7/2009)

Linkki:
https://vm.fi/documents/10623/307681/VAHTI+periaatep%C3%A4%C3%A4t%C3%B6s+2009/24355a33-4042-42fb-9dba-981e6398ee7a/VAHTI+periaatep%C3%A4%C3%A4t%C3%B6s+2009.pdf

Luonnos hallituksen esitykseksi eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi

Linkki:
https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=3010f613-2ede-40c1-a59f-e75c23cddbb5

Valtiovarainministeriön julkisen hallinnon digitaalisen turvallisuuden kokonaiskuva – ST IV

Euroopan Unionin yhteinen tiedonanto Euroopan parlamentille ja neuvostolle - Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle

Linkki:
https://publications.europa.eu/fi/publication-detail/-/publication/15499d93-794f-11e3-b889-01aa75ed71a1/language-fi

Kyberturvallisuuden uudistus Euroopassa
https://www.consilium.europa.eu/fi/policies/cyber-security/

EU leaders agree on ground-breaking regulation for cybersecurity agency ENISA
https://www.enisa.europa.eu/news/enisa-news/eu-leaders-agree-on-ground-breaking-regulation-for-cybersecurity-agency-enisa

Suomen Kyberturvallisuusstrategia sekä toimeenpano-ohjelma vuosille 2017 – 2020

Linkki:
https://www.turvallisuuskomitea.fi/index.php/fi/mcdc/14-suomen-kyberturvallisuusstrategia

https://www.turvallisuuskomitea.fi/index.php/fi/component/k2/126-suomen-kyberturvallisuusstrategian-toimeenpano-ohjelma-2017-2020

Valtiontalouden tarkastusviraston tarkastuskertomus - Kybersuojauksen järjestäminen

Linkki:
https://www.vtv.fi/files/5862/16_2017_Kybersuojauksen_jarjestaminen.pdf

Valtioneuvoston selvitys- ja tutkimustoiminta - Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi

Linkki:
http://tietokayttoon.fi/hankkeet/hanke-esittely/-/asset_publisher/suomen-kyberturvallisuuden-nykytila-tavoitetila-ja-tarvittavat-toimenpiteet-tavoitetilan-saavuttamiseksi

Valtioneuvoston selvitys- ja tutkimustoiminta - Kyberturvallisuuden strateginen johtaminen Suomessa

Linkki:
http://tietokayttoon.fi/hankkeet/hanke-esittely/-/asset_publisher/kyberturvallisuuden-strateginen-johtaminen-suomessa

EU:n yleinen tietosuoja-asetus

Linkki:
http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC

YTS 2017

Linkki:
https://www.turvallisuuskomitea.fi/index.php/fi/yhteiskunnan-turvallisuusstrategia-yts

Valtiontalouden tarkastusviraston tarkastuskertomus - Sähköisten palvelujen toimintavarmuuden ohjaus

Linkki:
https://www.vtv.fi/files/5863/15_2017_Sahkoisten_palvelujen_toimintavarmuuden_ohjaus.pdf

Valtioneuvoston päätös huoltovarmuuden tavoitteista 5.12.2018.
https://tem.fi/paatos?decisionId=0900908f805f483d

Toimittaja:
Kimmo Rousku

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 VALTIONEUVOSTO
Puhelin 0295 160 01
www.vm.fi

ISSN 1797-9714 (pdf)
ISBN 978-952-251-975-7 (pdf)

Joulukuu 2018